



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,408	05/25/2000	Lynn Spraggs	PA1066US	1972

7590 03/01/2004

Lynn Spraggs
Ultra Information Systems, LLC
8604 Kalavista Drive
Vernon B.C., V1B 1K3
CANADA

EXAMINER

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

7

DATE MAILED: 03/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/555,408

Applicant(s)

SPRAGGS, LYNN

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 May 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-5, 8-12, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Massey et al (US-4567600).

As per claims 1, 3, 9, and 15, Massey et al disclose a method and apparatus for public key exchange in a cryptographic system. Massey et al disclose a method of exchange file M from the user J and user K (Col 5 lines 1-5). The message M will be raised to the power of two random numbers, E_j and D_j of User J and E_k and D_k of User K. When user J send the message to user K, the message get raised to the power of first random integer E_j , $Y_1 = M^{E_j}$ (Col 5 line 15). User K raises the message to the power of E_k , $Y_2 = Y_1^{E_k}$ (Col 5 line 29), then pass the message back to user J. User J raises message to the power of the second random number D_j , i.e. $Y_3 = Y_2^{D_j}$ (Col 5 line 60). The message will be passed back to User K to raise the power of D_k to the message, i.e. $Y_4 = Y_3^{D_k}$ (Col 6 line 33). The math calculation in Col 5 and 6 finalize the result to the message M, which means that $Y_4 = Y_3^{D_k} = M$, the original message. Encrypting and Decrypting are math calculation done on the data file. Since either party does not know E_j and D_j or E_k and D_k , E and D are considered as private key. In Massey et al

invention, it is clear that the E representing encryption and D representing Decryption. Therefore, it is obvious at the time the invention was made for one of ordinary skill in the art to recognize that Massey et al teach the applicant invention completely.

As per claims 4, 10, and 16, Massey et al disclose the method of claims 3, 9 and 15, further including the step of storing the unsecured data on the second computer. It is obvious at the time the invention was made for one of ordinary skill in the art to see that a memory must exist in the system.

As per claims 5, 6, and 11, Massey et al disclose the method of claims 3 and 9, further including the step of verifying the validity of the unsecured data after decrypting the third encrypted data file at the second computer. It is obvious at the time the invention was made for one of ordinary skill in the art to see that the validity of the message is in the system, since the message get verified by the receiver every time before the user encrypt or decrypt the message (Col 5 lines 20-25).

As per claims 8, 12, and 14, Massey et al disclose the method of claim 9, wherein the encrypting and decrypting is performed using associative properties of encryption and decryption. It is obvious at the time the invention was made for one of ordinary skill in the art to recognize that the system is using the associative properties of encryption and decryption. The evidence is clear that both side do multiply (Col 5 Equation 3) by an

integer E and divide (Col 5 lines 50-53) by an integer $D=E$ to have the original result.
This is nothing more than a math equation.

Claims 2, 7, and 13 are rejected under 35 U.S.C 103(a) as being unpatentable over Massey et al (US-4567600), in view of Soutar et al (US-6219794).

As per claim 2, 7, and 13, Massey et al discloses the system in claim 1, 3, 9, and 15 completely. However Massey et al do not teach the use of biometric info as the private key. However, Soutar et al disclose "A method for secure key management using a Biometric" invention, which includes the method and system fully (Col 3 lines 38-46). It is obvious at the time of the invention for one of ordinary skill in the art to incorporate the biometric digitized key into a private key system to enhance the uniqueness of the key to maximize the security in the communication channel.

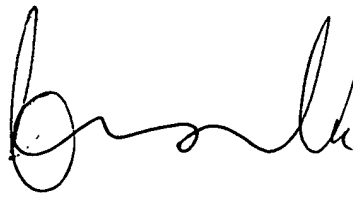
Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
2. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.
3. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax

numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son

Patent Examiner



CONFIDENTIAL
TECHNICAL INFORMATION